Michigan Senate Energy & Technology Committee (Sen. Mike Nofs - Chairperson):

Members of the Energy and Technology Committee,

I was asked to provide brief testimony on the status of cyber security within Financial Institutions. While it is my opinion that the financial sector has done better than most in protecting its data and other assets, there is one thing I am sure of, there is no silver bullet when it comes to security. To that end one thing is certain. As long as there is a profit to be made, criminals will never give up trying to find ways to circumvent security measures meant to protect data.

Since the 1930's financial institutions have worked very hard to build and maintain a level of trust most Americans have simply come to expect. In addition, laws like the Gram Leach Bliley Act of 1999 and other regulations, financial institutions have invested in and deployed numerous approaches to keep non public information from falling into the wrong hands. These approaches range from investments in technology, policy, procedure and training. All of which are deployed in a layered approach. If one control is compromised a second, third or fourth would potentially alert the institution that something isn't as it should be. There is no silver bullet.

While financial institutions appear to have a lot going right, that isn't always the case for its customers. Over the past few years it has become clear to criminals that it is easier to compromise the customer than it is the financial institution. Specifically, businesses are the main target as they have access to online systems that provide a vehicle to move thousands to millions of dollars out of the financial institution. Malware compromises the businesses PC and the very machine used to conduct normal business with the financial institution is utilized with the business users very own credentials to carry out ACH and or wire instructions to move money out of their business accounts.

Throughout 2013 there were multiple security events that grabbed the attention of the media. The top of most journalists list would have to be Edward Snowden. As you likely recall, Snowden had copied anywhere from 50,000 to 200,000 NSA documents. Later estimates ran as high as 1.7 million. Adobe's security breach allowed 3 million encrypted credit card records as well as an undetermined number of user account credentials. The initial report stated 38 million, but a file posted by AnonNews.org appeared to contain 150 million usernames and the corresponding hashed passwords. Similar breaches were disclosed by Target and Neiman Marcus. In both cases these major retailers breach of security allowed criminals to abscond with customer information. Target purportedly leaked 40 million U.S. credit and debit cards and personal information on about 70 million customers. Neiman Marcus has yet to fully disclose those impacted and exactly what information was taken, but their press release seems to indicate they are mostly concerned with customer credit and debit card information.

Card issuers are now faced with choosing to replace the identified credit and or debit cards of its impacted customers or maintain expensive systems to monitor those cards especially close. Either way card issuers are spending money to clean up the mess and protect themselves from further losses. Often times losses from card fraud rise just before a major announcement like that of Target and Neiman Marcus breaches. Then you have the impact on customers. Some consumers could end up being impact multiple times in a year. This obviously starts to be a major inconvenience and deteriorates their trust. Some have been impacted so many times already that they are numb to the process.

How is it that these types of breaches happen? Sometimes it is a poorly configured or un-patched web server that is breached by a SQL injection attack. In other cases it is an inside job for money or political reasons. In a lot of situations it is inadvertent human behavior that allows the compromise to happen. The one common thread here is the human element. No matter what security controls are in place, the human element is always the weakest link. You can spend hundreds of thousands on security and have one person within the organization click a link inside an unsolicited email promising they won a free all expenses paid trip, Ipad, you name it and your expensive security was just compromised. An employee finds a USB thumb drive in the parking lot, inserts it into their work machine and your security investment was just compromised.

So what do we do about this? Financial institutions will continue to deploy new technology, policies, and procedures in a layered approach as they always have. In addition, we will continue to educate our customers as best we can to help them understand how their own security and employee training programs are just as important. When working with customers that have had a breach, I like to remind them to not only focus on the attempted financial transactions, but what other assets do they have that the criminals might try to take. Their employee and customer records are potentially as much of a target as the financial institution systems.

How can the State help? One way might be to assist with the training efforts of consumers and business owners alike. Electronic systems can be utilized for so much good. But as we know, it can be used by those with bad intentions. We cannot train, retrain and train some more the people of Michigan. This needs to happen at the State level all the way down to parents and teenagers. Everyone is involved whether they like it or not, whether they realize it or not. It amazes me how many people freely give up their private information on Facebook or have individuals become so numb to their data being leaked that they just don't care?

Another way the State may be able to help is to appropriate an appropriate amount of the budget on technology that will protect not only the State but its residents. Continue to build on the task forces that monitor, track and investigate those that choose to attack Michigan residents and businesses from the comfort of their home, wherever that is. Like Microsoft, the State needs to take as much of an offensive stance as it does a defensive one. I have had the privilege of hearing Dan Lohrmann speak on numerous occasions and was pleased to hear how the security programs being implemented by the State of Michigan are being copied elsewhere. We encourage the State to continue to make investments in this area. The State of Michigan needs to be and should be a leader in this space.

Lastly, how does the State react to the apparent trend in attacking retailers? PCI-DSS has been around for a number of years. Does that standard have the appropriate controls in it? Are the audits and oversight of that industry appropriate? We know if the financial sector had these types of announcements, the media would have a heyday. We hope that day never comes.

In closing, there is always room to do more. Security will never be a set it and forget it thing. We hope the State will join in and be a part of the security solution by protecting as well as helping educate Michigan businesses and citizens on how best to protect themselves. As mentioned earlier, we are all in this together.